

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
28 June 2001 (28.06.2001)

PCT

(10) International Publication Number
WO 01/46923 A1

(51) International Patent Classification⁷: **G08B 13/24**,
15/00, G07C 9/00

(21) International Application Number: PCT/US00/42802

(22) International Filing Date:
11 December 2000 (11.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/469,644 22 December 1999 (22.12.1999) US

(71) Applicant: **AXCESS INC.** [US/US]; 3208 Commander
Drive, Carrollton, TX 75006 (US).

(72) Inventor: **GRIEBENOW, Allen, R.**; 5419 Preston Fair-
ways Circle, Dallas, TX 75252 (US).

(74) Agent: **STALFORD, Terry, J.**; Baker Botts L.L.P., 2001
Ross Avenue, Dallas, TX 75201-2980 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AT
(utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA,

CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility
model), DK, DK (utility model), DM, DZ, EE, EE (utility
model), ES, FI, FI (utility model), GB, GD, GE, GH, GM,
HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,
LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX,
MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK
(utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN,
YU, ZA, ZW.

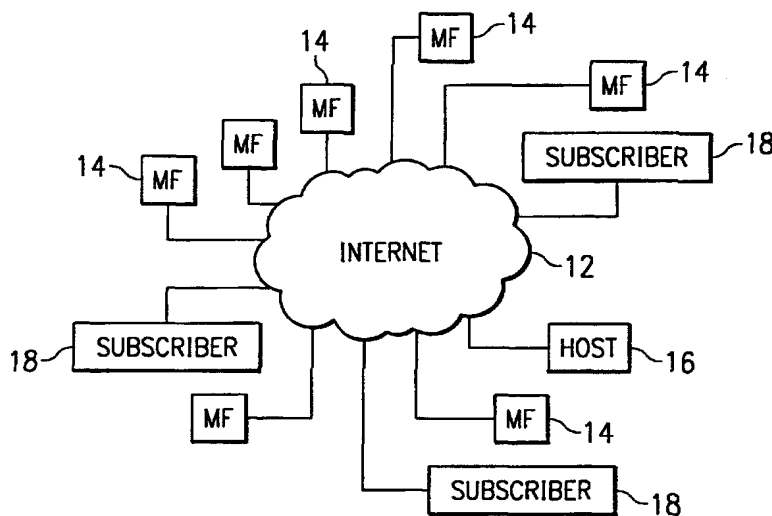
(84) Designated States (*regional*): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian
patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European
patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,
IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF,
CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

- With international search report.
- Before the expiration of the time limit for amending the
claims and to be republished in the event of receipt of
amendments.

For two-letter codes and other abbreviations, refer to the "Guid-
ance Notes on Codes and Abbreviations" appearing at the begin-
ning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR PROVIDING INTEGRATED REMOTE MONITORING SERVICES



(57) Abstract: A method and system for providing integrated remote monitoring services includes receiving and storing radio frequency identification (RFID) data from an RFID system at a remote facility of a subscriber. Video data is received from a video system at the facility and also stored. The subscriber is provided with access to the stored RFID and video data. The subscriber is also provided with access to and control of a video camera in the video system at the facility.



WO 01/46923 A1

METHOD AND SYSTEM FOR PROVIDING INTEGRATED REMOTE
MONITORING SERVICES

TECHNICAL FIELD OF THE INVENTION

The present invention relates generally to the field of remote business management, and more particularly to a method and system for providing integrated remote
5 monitoring services.

BACKGROUND OF THE INVENTION

Remote monitoring of a facility for fire, burglar and other alarms provides protection for a facility at
10 low cost. For fire alarm systems, heat, flame, and/or smoke sensors are strategically placed around the facility to detect any fire at an early stage. Upon detection of a fire, in addition to a local alarm, an alarm is sent to a remote monitoring facility, which can
15 then notify the fire department.

Similarly, homes and businesses often have a burglar alarm that is remotely monitored. Typically, sensors are placed on doors, windows, and at other areas susceptible to forced entry. In response to detection of a break-in,
20 an alarm is sent to the remote monitoring facility, which can then dispatch personnel to check the facility.

A significant problem in monitoring alarms is the occurrence of false alarms. For burglar alarms, for example, personnel must generally be dispatched to the
25 scene to determine whether a break-in is actually occurring or has occurred. In the event of a break-in, the need to confirm the alarm delays notification of the

police. In the event no break-in occurred, the false alarm unnecessarily diverts personnel and resources to the scene.

More recently, remote monitoring capabilities have improved with the advent of video telesurveillance technologies. This technology allows remote personnel to connect to a video camera in a facility and to control or determine conditions at the facility. While this remote "look-in" capability provides significant advances over earlier monitoring systems, it does not provide an integrated solution for business owners.

SUMMARY OF THE INVENTION

The present invention provides a method and system for providing remote monitoring services that substantially reduce or eliminate the problems and disadvantages associated with previously developed systems and methods. In particular, the present invention provides integrated remote monitoring services that allow a subscriber to remotely monitor, evaluate, and control operations at a facility.

In accordance with one embodiment of the present invention, a method and system for providing integrated remote monitoring services includes receiving and storing radio frequency identification (RFID) data from an RFID system at a remote facility of a subscriber. Video data is received from a video system at the facility and also stored. The subscriber is provided with access to the stored RFID and video data. The subscriber is also provided with access to and control of a video camera in the video system at the facility.

More specifically, in accordance with a particular embodiment of the present invention, the RFID and video information may be received over the Internet and the

subscriber provided access to the stored data and the video camera through a web portal. In this and other embodiments, the RFID data may be processed to generate a report for the subscriber or to determine and notify the subscriber of any alert conditions requiring his or her attention. In addition, the subscriber may initiate a polling event at the facility and receive results of the polling event.

In accordance with another aspect of the present invention, a method and system for providing identity verification for access activities is provided. The method and system elicits a radio response from an RFID tag at an access door of a secure area. Authorized access by a wearer of the RFID tag to the secure area is determined based on the radio response. A video image of the wearer at the access door is recorded and used to confirm the identity of the wearer.

In accordance with still another aspect of the present invention, a method for providing remote access services includes receiving a request by a person for access to a restricted area operated by a subscriber. A video image of the person requesting access to the restricted area and/or RFID tag information is also received. The request, including the video image, is transmitted to the subscriber for approval. In response to approval by the subscriber, the requested access is remotely allowed.

Technical advantages of the present invention include providing integrated remote monitoring services for owners and managers of a business. In particular, data is collected from the facility using automatic location identification technology and digital video networking and recording technology. The data is transmitted over the Internet to a central host site at

which the data is stored and analyzed and may be accessed by the subscriber.

Another technical advantage of the present invention includes using the Internet to provide multi-media and other data-oriented information to subscribing business managers that is specific to the operation of each business location for the purpose of improving the efficiency of business operations. In particular, video, audio, and other data is collected at a business location and may be viewed live, processed, and stored at the business location or retrieved and processed at a central host site. The user subscribes to the service, which makes available the collected and processed data through a website portal.

Yet another technical advantage of the present invention includes providing video verification of activity at a remote facility. In particular, video images are collected and associated with radio frequency identification (RFID) activities. As a result, the identity of a person wearing or otherwise using a tag to access facilities, operations, and areas may be verified.

Still another technical advantage of the present invention includes providing a method and system for remotely notifying a manager of a facility of an alert condition at the facility. In particular, RFID data is collected and processed at a facility to determine whether a user-defined or other alert condition exists. Alert conditions may be unauthorized access to an area, an insufficient number of employees at the facility or performing a specified task, or other conditions that affect operations of the business. The manager is immediately notified of such alerts to allow corrective action to be taken.

Still another technical advantage of the present invention includes providing a method and system for providing remote access services to a subscriber. In particular, request by a person to access a restricted
5 area during off-hours or other unattended times is combined with RFID data, if available, and a video image and forwarded to a central host site for approval or routing to a subscriber for his or her approval. As a result, employees need not travel to or wait at a
10 location for deliveries or the arrival of others. Thus, operating costs of the business are reduced.

Still another technical advantage of the present invention includes providing a method and system for gathering marketing and customer preference information.
15 In particular, remote controlled cameras at a store may be accessed and controlled to determine customer preferences and actions. As a result, travel to the physical location is unnecessary which reduces costs and increases the number of surveys that can be taken. In
20 addition, interference with normal operations of a facility are eliminated.

Other technical advantages of the present invention will be readily apparent to one skilled in the art from the following figures, description, and claims.

25

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and its advantages, reference is now made to the following description taken in conjunction with the
30 accompanying drawings, wherein like reference numerals represent like parts, and in which:

FIGURE 1 is a block diagram illustrating a remote monitoring system in accordance with one embodiment of the present invention;

FIGURE 2 is a top plan view of a monitored facility of FIGURE 1 in accordance with one embodiment of the present invention;

FIGURE 3 is a block diagram illustrating details of the central host of FIGURE 1 in accordance with one
5 embodiment of the present invention;

FIGURE 4 is a flow diagram illustrating a method for providing identity verification service for a subscriber of the monitoring system of FIGURE 1 in accordance with
10 one embodiment of the present invention;

FIGURE 5 is a flow diagram illustrating a method for providing alert notification services for a subscriber of the monitoring system of FIGURE 1 in accordance with one embodiment of the present invention;

FIGURE 6 is a flow diagram illustrating a method for providing remote access services for a subscriber of the monitoring system of FIGURE 1 in accordance with one
15 embodiment of the present invention; and

FIGURE 7 is a flow diagram illustrating a method for providing location control services for a subscriber of the monitoring system of FIGURE 1 in accordance with one
20 embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

FIGURE 1 illustrates a remote monitoring system 10
25 in accordance with one embodiment of the present invention. In this embodiment, the remote monitoring system 10 uses the Internet to provide connectivity between remote elements of the system 10. It will be
30 understood that other suitable networks and components of networks may be used as part or in place of the Internet 12 to provide connectivity between elements of the system 10.

Referring to FIGURE 1, the remote monitoring system includes geographically distributed monitored facilities (MF) 14, a central host 16, and subscribers 18. The monitored facilities 14 each include a data collection
5 system that collects video, audio, location, and other data at the facility 14 based upon the specific business needs of a subscriber 18. The data, once collected, may be viewed live, processed and stored at the monitored facility 14, or retrieved and processed at the central
10 host 16. The subscriber 18, which may be an owner or manager of the business, accesses certain live and processed data relative to the operation of the facility 14 through a website portal defined by the central host 16. The subscriber 18 may access the website portal with
15 a personal computer or any other suitable personal device capable of connecting to the Internet through a wireline, wireless or other suitable link.

FIGURE 2 illustrates details of a monitored facility 14 in accordance with one embodiment of the present
20 invention. In this embodiment, the monitored facility 14 is a retail clothing store 40. It will be understood that the present invention may be used in connection with any other suitable type of business. For example, the monitored facility 14 may be any type of store selling
25 goods to consumers, a doctor or other suitable type of office, an office building or complex, a manufacturing facility or plant, a warehouse or storage yard, or any other suitable structure at which one or more workers perform tasks.

30 Referring to FIGURE 2, the retail store 40 includes a sales floor 42 and the back area 44 supported by a security door 46. The sales floor 42 is accessed by the public through access doors 48. The sales floor 42 includes clothing shelves 50, clothing racks 52, and a

sales counter 54. The clothing shelves and racks 50 and 52 display articles of clothing to consumers for selection and purchase, and dressing rooms 58. Typically, clothing is displayed on the shelves 50 and
5 racks 52 to maximize consumer interest and purchases. Such purchases are rung up by employees of the store on registers 58 at the sales counter 54. Money, checks, and receipts for other forms of payment are all initially stored in the registers 58.

10 The back area 44 includes a stock area 60, a vault room 62, and a computer room 64. The stock area 60 stores inventory 70 for later display on the sales floor 42. The vault room 62 secures a safe 72 that temporarily stores funds removed from the registers 58 prior to
15 transfer to a bank. The computer room 64 secures burglar and fire alarm equipment 74 and 76 as well as a local computer system 78 for monitoring, controlling, processing, recording, local activities and for transmitting and receiving information to and from the
20 central host 16. Local processing of data may be completely performed by the local computer system 78 or may be distributed to the sensors or other devices throughout the store 40. In the Internet embodiment, the computer system 78 includes a local area network (LAN)
25 hub/gateway to communicate with the central host 14 over the Internet 12. The vault and computer room 62 and 64 are each accessed by access doors 80 and 82, respectively.

The computer system 78 collects data using automatic
30 location identification technology and digital video networking and recording technology. In one embodiment, the automatic location identification technology comprises radio frequency identification (RFID) tag technology that gathers data by requiring assets to

physically touch a reader (passive location technology) or by passing near to a reader (active location technology). Active tags activate, or wake-up when they pass through or receive a localized radio frequency signal and then transmit their ID number to a reader. The RFID data identifies where certain personnel or physical assets of the business are or have been in or around the store 40. The RFID data is collected as the assets enter or leave the store 40 and as they move into or out of certain defined areas, or zones.

In a particular embodiment, the RFID system and tags may be implemented in accordance with the systems and tags disclosed in U.S. Application Serial No. 09/298,982 that is entitled "Distributed Tag Reader System and Method", U.S. Application Serial No. 09/357,435 that is entitled "Radio Frequency Identification System and Method", U.S. Application Serial No. 09/298,559 that is entitled "Low Power Receiver for Radio Tag and Method", U.S. Application Serial No. 09/258,974 that is entitled "High Sensity Demodulator for a Radio Tag and Method", U.S. Application Serial No. 08/789,148 entitled "Radio Tag System and Method With Improved Tag Interference Avoidance", U.S. Application Serial No. 09/357,669 entitled "Dual Frequency Radio Tag for Radio Frequency Identification System, and U.S. Application Serial No. 09/357,688, all of which are incorporated herein by reference.

For the illustrated embodiment, the store 40 includes a centralized receiver, or reader, 90 for reading responses from tags, access control systems 92 for controlling access to the back area 44 and an access monitoring system 94 for monitoring tags entering through the public doors 48. The access control and monitoring systems 92 and 94 each transmit the wake-up signal to

tags in their area to elicit a response which is received by the receiver 90 and passed to the computer system 78. In this way, access to the back area 44 may be fully controlled with only authorized personnel having an RFID tag allowed access. Thus, while the general public may freely access the sales floor 42, access to the back room 44 is limited to only employees and managers of the store 40. Inclusion of the access monitoring system 94 allows the egress and ingress of all employees entering or leaving the store 40 to be monitored and recorded.

Additional access control systems 96 and 98 are provided separately for the vault room 62 and the computer room 64 to provide additional security to those areas. Thus, while all employees may be allowed access to the back area 44, only specific employees or an owner may be allowed access to the vault room 62 and the computer room 64.

The location data may also include polling stations 100 and 102. The polling station 100, in response to a command from the local computer system 78 polls tagged inventory on the sales floor 42. Responses from the tags may be collected by the polling station 100 or the receiver 90 and forwarded to the local computer system 78 for processing. Similarly, polling station 102, in response to a command from the local computer system 78, may poll tagged items in the inventory 70. Responses from the tags may be received by the polling station 102 or the receiver 90 and passed to the computer system 78 for recordation and processing. Typically, high value items will be tagged to inhibit their theft. The computer system 78 may initiate polling at specified times, at a specified period, in response to an alarm condition, or in response to an operator or subscriber request from or through the central host 16.

The location data may be recorded at the store 40 and transmitted later or transmitted live over the Internet 12 where it is collected by the central host 16, processed, and then made available to the subscriber 18.

5 In one embodiment, the RFID data may include the identification number of the tag, the antenna or activator ID telling where the tag was activated, and the reader identification that received the response signal from the tag.

10 The video and audio data at the store 40 is collected from cameras and microphones positioned in and around the store 40. The video may be black and white video, color video, infrared video, or any other suitable visual information capable of providing information at a scene. The cameras may be digital network video cameras, which can connect directly to a data network, or they may be any standard video camera connected to a conversion and compression device, which records and/or prepares the video data for transmission over the Internet 12.

20 The video data collection and/or transmission may be initiated via an external trigger or alarm which indicates a business condition exists where the video data must be transmitted live or recorded for later review. Video data is also available for subscribers 18 or the host service provider 16 to dial into at any time to view live video or to initiate video recording. In addition, Video data may be recorded at the store 40 and transmitted later or transmitted live over the Internet 12 or may be recorded the central host 16 or transmitted live to the subscriber 18.

In one embodiment, the cameras and equipment of the video and audio network may be implemented in accordance with U.S. Patent No. 4,857,991 entitled "Method and System for Decompressing Color Video Feature Encoded

Data", U.S. Patent No. 4,816,901 entitled "Method and System for Compressing Color Video Data", U.S. Patent No. 4,843,466 entitled "Method and System for Decompressing Color Video Slope Encoded Data", U.S. Patent No. 5 4,849,807 entitled "Method and System for Compressing Color Video Feature Encoded Data", U.S. Patent No. 4,847,677 entitled "Video Telecommunication System and Method for Compressing and Decompressing Digital Color Video Data", U.S. Patent No. 4,857,993 entitled "Method and System for Decompressing Digital Color Video Statistically Encoded Data", U.S. Patent No. 4,914,508 10 entitled "Method and System for Compressing and Statistically Encoding Color Video Data", U.S. Patent No. 5,140,142 entitled "Method for Color Encoding and Pixelization for Image Reconstruction", U.S. Patent 15 Application Serial No. 07/611,142 entitled "Data Processing Apparatus and Method Using Data Compression (Delta)", U.S. Patent Application Serial No. _____ filed on March 20, 1998 entitled "Conditional Update Method for Video Compression", U.S. Patent Application 20 Serial No. _____ filed March 20, 1998 entitled "Video Compressed Apparatus and Method, and U.S. Patent Application Serial No. 08/610,618 which are all hereby incorporated by reference.

25 For the illustrated embodiment, video and audio data are collected by a number of digital cameras distributed throughout the store 40. Each camera includes a camera controller (CC) for panning, tilting, and zooming the camera to focus on a desired area of the store 40. In 30 particular, sales floor cameras 110 and 112 provide broad coverage of the sales floor 42 and may be used to view the movements of customers and interaction between customers and employees on the sales floor 42. A sales counter camera 114 is located in front of the sales

counter 54 to provide close-up coverage of the registers 58. In the back area 44, camera 116 provides coverage of a back door, camera 118 provides coverage of the intermediate door 46 between the back area 44 and the sales floor 42, vault camera 120 provides coverage of the vault door 80, and computer camera 122 provides coverage of the computer door 82. Thus, all access to the back room 44 and the vault and computer rooms 62 and 64 may be recorded. In addition, back area camera 124 may provide broad coverage of the stock area 60.

Video, audio, location, and other data gathered by the sensors in the store 40 are passed to the local control system 78 for recordation, processing, and transmittal to the central host 16. The local computer system 78 may combine location data with multi-media data to provide enhanced and integrated services for subscribers 18. In a particular embodiment, data is streamed out of the location and video system. The location data is embedded into video frame headers for transmission and storage.

Combined location and video data may be generated in an application in which tag transmissions may be used to active video recording from a camera pointed toward a zone activation point to capture tag activations. The video records the tagged activation event thereby validating the person or asset with a tag at the time of the read. The combined tag and video data can be stored for later review or transmitted live over the Internet to the central host 16 or to the subscriber 18.

FIGURE 3 illustrates the central host 16 in accordance with one embodiment of the present invention. In this embodiment, the central host 16 is implemented as a website portal on a server. It will be understood that the host 16 may be implemented by any other suitable

computing device capable of communicating information with a remote device over a network.

Referring to FIGURE 3, the host 16 includes database 150 for storing data received from the monitored facilities 14 and applications 152 for processing the data and reporting the information to the subscribers 18. Generally described, the central host 16 receives, stores, and processes video, audio, and location data transmitted from the monitored facilities 14 and makes the data available to the subscribers 18. In addition, the host 16 may generate and transmit notice of certain events to the subscriber 18.

The database 150 includes activity records 160 for each of the monitored facilities 14. The activity records 160 each store location information 162, video information 164, and combined location and video information 166. The location information 162 is generated by RFID reads at the monitored facilities 14. The location data 160 may include time and attendance records, access to restricted areas information, asset movement information, and asset poll results. The time and attendance records provided to the subscriber 18 to automate the payroll data input process, to counsel an employee regarding deficiencies in his or her attendance, and combined with video data to provide a video record of attendance. Access to restricted area information allows the subscriber to track personnel entering inventory rooms, computer rooms, rooms with safes and other critical areas of a facility 14. The asset movement data provides subscribers with information regarding unauthorized movement of assets. The poll results provide subscribers an inventory of tag assets at a particular facility 14.

The video data 164 may include associated audio clips and is generated by the cameras at the monitored facilities 14. The video data may include video of personnel entering and leaving a monitored facility 14, personnel movement within the facility 14, customer video and purchase transaction video. Personnel access video may be provided to a subscriber 18 as a record of authorized and unauthorized entry by employees and non-employees. Personnel movement video data may be used by the subscriber 18 to evaluate the effectiveness of an employee at his or her job functions. Such functions can include performance of job tasks, interaction with customers, and behavior involving customer transactions such as cash handling. Customer video data may be used by subscribers 18 to provide information regarding customer behavior in buying circumstances such as attractiveness to product displays. The register transaction videos provide protections for the subscriber against theft.

The combined format data 166 stores location and video information together to provide enhanced services and higher order information for subscribers 18. Location and video information may be stored together by being stored in a common file, by being stored in a common element of a database, or being linked or otherwise associated with each other.

The applications 152 include a facility access program 180, database access program 182, alert processor 184, report generator 186, remote video controller 188, remote access controller 190, and remote location, or RFID, controller 192. The applications each comprise software stored on a computer-readable medium and executed by a processor of the host 16. It will be understood that the functionality of the central host 16

may be otherwise suitably separated into disparate applications.

The facility access program 180 provides operators and subscribers 18 with direct access to the local
5 computer system 78 of the monitored facilities 14. The database access program 182 provides access to the database 150. Accordingly, an operator at the central host 18 can perform special requests and processing of information stored at the central host 18 or at the
10 monitored facility 14.

The alert processor 184 receives alerts generated by the monitored facilities 14 and/or generates alerts and response to information uploaded from the monitored facilities 14. As described in more detail below, the
15 alert processor notifies the subscribers 18 of an alert condition in order to allow them to suitably respond. The alerts may be a burglar alarm, a fire alarm, or subscriber-defined operation conditions such as less than a minimum number of employees at a facility or performing
20 a specified function at a facility.

The report generator 186 processes information in the activity records 160 to generate user-required and/or specified reports. The reports allow a subscriber to quickly determine the operational status of a monitored
25 facility 14 based on certain categories of information. The reports can be accessed on the central host 16 or transmitted to the subscriber 18.

The remote video controller 188 provides operators and subscribers 18 with direct access to and control of
30 the video cameras in the monitored facilities 14. Thus, an operator may look into any of the monitored facilities 14 at any time. Typically, an operator would use the remote video controller 188 to look into a monitored facility 14 in response to an alarm or other alert

condition. In one embodiment, the remote video control 188 is implemented as the prism MOLE software. The MOLE application allows full pan, tilt, and zoom camera control. In addition, the MOLE product supports black and white, color, and infrared video images and provides
5 an intuitive graphical user interface (GUI) for remotely controlling the cameras.

The remote access controller 190 provides operators and subscribers with remote access functionality at the
10 central host 16. As described in more detail below, this enables an operator at the central host 16 to control access doors at the monitored facilities 18 to allow ingress and egress of employees and other personnel. This subscriber 18 may use the remote access controller
15 190 to similarly control access doors at the monitored facility 18. The doors at monitored facilities 14 may include gates and other entry and exit ways.

The remote RFID controller 192 allows operators and subscribers to access and control an RFID system, or
20 components of an RFID system at a monitored facility 14. For example, an operator at the central host 16 or a subscriber 18 may initiate polling operations at a monitored facility to track inventory at that facility 14. In this way, inventory may be remotely polled on a
25 periodic basis, at specified times, or at any random time by the subscriber 18.

The central host 16 implements an Internet website to allow subscribers 18 to connect to the host and view the location data, video data, and process result data.
30 In one embodiment, the subscriber 18 is given an authorization number to ensure privacy of the data being viewed. The website, or portal, may present options to the subscriber 18 for live video viewing at any location, viewing recorded video clips of key operational events,

viewing data from location reads such as time and attendance by employees and asset movements, and viewing data from asset inventory polls. The subscribers 18 may also receive e-mail alerts which may include alarm
5 messages of events that require immediate attention. The e-mail alerts may include video, snapshots, or clips of key events.

FIGURE 4 is a flow diagram illustrating a method for providing identity verification services to subscribers
10 18 for RFID reads at a monitored facility 14 in accordance with one embodiment of the present invention. The method begins at step 200 in which a radio response is elicited from an RFID tag at an access door of a secure area of a monitored facility 14.

15 Next, at step 202, one or more video images of the wearer of the RFID tag is obtained from a camera covering the access door. The video image may be obtained in response to the radio response, authorized access, or an attempt at unauthorized access.

20 Proceeding to decisional step 204, it is determined if the requested access is authorized based on the radio response from the RFID tag. If access is authorized, the Yes branch of decisional step 204 leads to step 206 in which the access door is opened. If access is not
25 authorized, the No branch of decisional step 204 along with step 206 leads to step 208.

At step 208, the video image is stored with the RFID action to provide video verification of the event. The video image may be stored with the RFID action by being
30 stored as part of a same file, database entry, linked, or otherwise associated with the action.

FIGURE 5 illustrates a method for providing an alert notification service to subscribers 18 in accordance with one embodiment of the present invention. In this

embodiment, the alert is initially generated at a monitored facility 18 by a local computer system and transferred to the central host 16 for processing and transmittal to the subscriber 18. It will be understood
5 that the alert may be generated by the central host 16 based on received and processed data. In this embodiment, information relevant to the alerts is preferably streamed from the monitored facilities 14 to the central host 16 for continuous processing.

10 Referring to FIGURE 5, the method begins at step 250 in which a location or other RFID event is received at a monitored facility 14. Next, at decisional step 252, it is determined whether the event is associated a pre-defined alert condition. The alert condition may be a
15 burglar or fire alarm, or operational data above or below operational limits. If the event is not associated with an alert condition, no immediate notification to the subscriber 18 is necessary and the No branch of decisional step 252 leads to the end of the process. If
20 the event is associated with an alert condition, the Yes branch of decisional step 252 leads to step 254.

At step 254, a video image providing information about the RFID event may be obtained. The video image may be obtained by triggering a camera covering an area
25 in which the RFID event occurred or by retrieving video recorded at the time of the event. Next, at step 256, notice of the alert and any attached video images are transmitted to the central host 14 for processing.

Proceeding to step 258, the alert processor 184 at
30 the central host 16 generates an e-mail to the subscriber providing notice of the alert condition. For example, the e-mail may include a textural message indicating the monitored facility 14 at which the event occurred, the type of the event, and the time of the event. At step

260, the video image is attached to the e-mail and the complete message transmitted to the subscriber 18 at step 262. In this way, subscribers 18 are immediately notified of any events to which immediate action may be required.

FIGURE 6 is a flow diagram illustrating a method for providing remote access services for subscribers 18 in accordance with one embodiment of the present invention. In this embodiment, requests for remote access are processed by the central host 16 and forwarded to the subscriber 18 for approval. It will be understood that an operator at the central host 16 may provide requested access based on instructions by the subscriber 18.

Referring to FIGURE 6, the method begins at step 300 in which a request by a person to access a restricted area is received at a monitored facility 14. At step 302, a video image of the person requesting access is obtained. The video image may be obtained by triggering the camera covering the access door from which the request was received.

Proceeding to step 304, the request and the video image are transmitted to the central host 16. At the central host 16, the remote access controller 190 generates an e-mail to the subscriber 18 providing notice of the request. At step 308, the video image is attached to the e-mail and the completed e-mail transmitted to the subscriber at step 310.

Next at decisional step 314, if the subscriber grants the request, the Yes branch leads to step 316 in which the access door is remotely opened. The door may be opened by the subscriber 18 via the central host 16 or by an operator at the central host 16 in response to approval of the request by the subscriber 18.

Step 316 as well as the No branch of decisional step 314 lead to the end of the process. In this way, after-hour deliveries and other access may be allowed without the need to maintain employees at a facility.

5 Accordingly, operational expenses for the business are reduced.

FIGURE 7 is a flow diagram illustrating a method for providing remote polling services for subscribers 18 in accordance with one embodiment of the present invention.

10 The method begins at step 350 in which a polling event is received for an area at a monitored facility 18. The polling event may be a specified time, the elapse of a period of time, or a response to a request by the subscriber 18 or an operator at the central host 16. In

15 addition, the polling event may be an RFID event within the area to be polled.

Next, at step 352, a poll is conducted of the area for tagged inventory. In accordance with conventional radio tag operations, each tag responds to a polling

20 event by identifying itself and providing any other relevant information. At step 354, the results of the poll are transmitted to the central host 16 for processing. Proceeding to decisional step 356, the central host 16 determines whether any inventory is

25 missing. This may be accomplished by comparing the inventory results to previous inventory results and accounting for any items for which removal was authorized, such as sold items. If no inventory is missing, no notification to the subscriber is needed and

30 the No branch of decisional step 356 leads to the end of the process. If inventory is missing, the Yes branch of decisional step 356 leads to step 358.

At step 358, the remote RFID controller 192 generates an e-mail to the subscriber 18 providing notice

of the missing inventory. At step 360, the controller 192 may attach a log of recent RFID activity in the area at which the missing inventory was discovered. The completed e-mail is transmitted to the subscriber 18 at
5 step 362. This way, a subscriber 18 may be immediately notified of any missing inventory and may take suitable action.

Although the present invention has been described with several embodiments, various changes and
10 modifications may be suggested to one skilled in the art. It is intended that the present invention encompass such changes and modifications as fall within the scope of the appended claims.

WHAT IS CLAIMED IS:

1. A method for providing integrated remote monitoring services, comprising:

receiving and storing radio frequency
5 identification (RFID) data from an RFID system at a remote facility of a subscriber;

receiving and storing video data from a video system at the facility;

providing the subscriber with access to the
10 stored RFID and video data; and

providing the subscriber with access to and control of a video camera in the video system at the facility.

15 2. The method of Claim 1, wherein the RFID and video information is received over the Internet and the subscriber is provided with access to the stored data and to the video camera through a web portal.

20 3. The method of Claim 1, further comprising processing the RFID data to determine whether an alert condition exists and notifying the subscriber if an alert condition exists

25 4. The method of Claim 3, wherein the alert is a subscriber-defined alert.

5. The method of Claim 3, further comprising generating an e-mail and transmitting the e-mail to the
30 subscriber to notify the subscriber of the alert condition.

6. The method of Claim 3, wherein the alarm condition comprises less than a minimum number of employees in attendance at the facility.

5 7. The method of Claim 3, wherein the alarm condition comprises less than a minimum number of employees performing a specified function.

8. The method of Claim 1, further comprising:
10 initiating a polling event in response to a specified event, the polling event operable to use the RFID system at the facility to poll an area of the facility to determine an inventory of tagged items within the area; and
15 receiving results of the polling event.

9. The method of Claim 8, wherein the specified event is a pre-defined time.

20 10. The method of Claim 8, wherein the specified event is a periodic event.

11. The method of Claim 8, further comprising:
determining whether all items have been
25 accounted for based on the polling results; and
generating an alert in response to unaccounted for items.

12. The method of Claim 1, further comprising
30 processing the RFID data to generate a report for the subscriber.

13. The method of Claim 12, wherein the report is a subscriber-defined report.

14. The method of Claim 12, wherein the report comprises time and attendance records of the employees of the subscriber at the facility.

15. A method for providing identity verification for access to a secure area, comprising:

eliciting a radio response from a radio frequency identification (RFID) tag at an access door of
5 a secure area;

determining whether access by a wearer of the RFID tag to the secure area is authorized based on the radio response;

recording a video image of the wearer of the
10 RFID tag at the access door; and

controlling access to the door to provide authorized access.

16. The method of Claim 15, further comprising
15 recording the video image in response to authorized access.

17. The method of Claim 15, further comprising
recording the video image in response to an attempt at
20 unauthorized access.

18. The method of Claim 15, further comprising
recording the video image in response to the radio
response from the RFID tag.

25

19. The method of Claim 15, further comprising
recording a series of video images of the wearer of the
RFID tag at the access door.

20. A method for remotely notifying a subscriber of an alert condition at a facility, comprising:

receiving a radio frequency identification (RFID) action from an RFID system at a facility;

5 determining whether the RFID action corresponds to a pre-defined alert condition;

obtaining a video image associated with the RFID action if the RFID action corresponds to a pre-defined alert condition; and

10 electronically transmitting notice of the alert condition along with the video image for delivery to a manager of the facility.

21. The method of Claim 20, further comprising
15 electronically mailing the notice of the alert condition along with the video image over the internet to the manager of the facility.

22. The method of Claim 21, further comprising
20 obtaining and electronically transmitting a series of video images associated with the RFID action.

23. The method of Claim 20, wherein the RFID action comprises access to a specified area.

25

24. The method of Claim 20, further comprising:

determining whether an expected RFID action has occurred by a specified time; and

30 electronically transmitting a notice that the expected RFID action has not occurred to the manager of the facility in response to determining that the expected RFID action has not occurred.

25. A method for providing remote access services, comprising:

receiving a request by a person for access to a restricted area operated by a subscriber;

5 receiving a video image of the person requesting access to the restricted area;

transmitting the request including the video image to the subscriber for approval; and

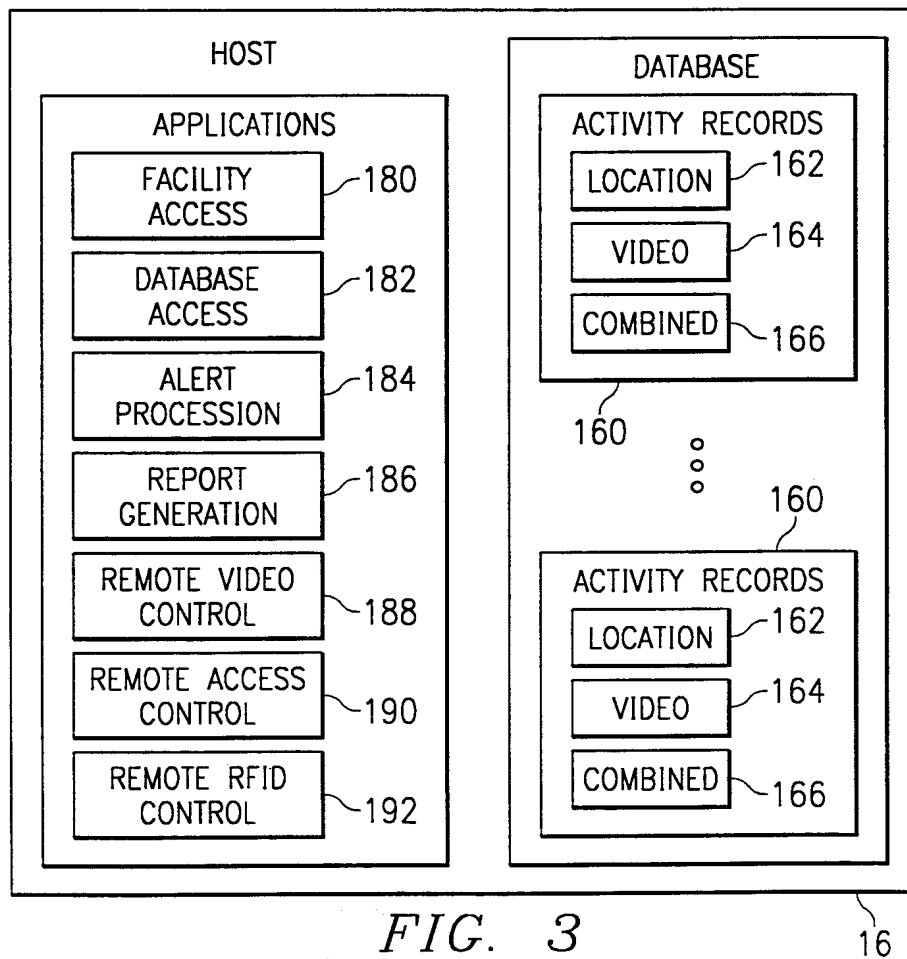
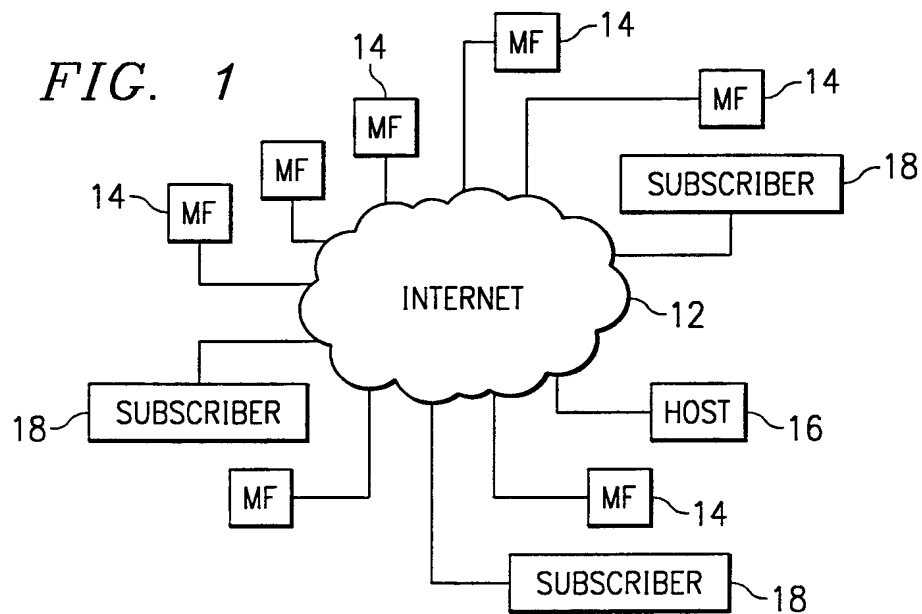
10 allowing the requested access in response to approval by the subscriber.

26. The method of Claim 25, further comprising receiving and transmitting a series of video images of the person requesting access to the restricted area.

15

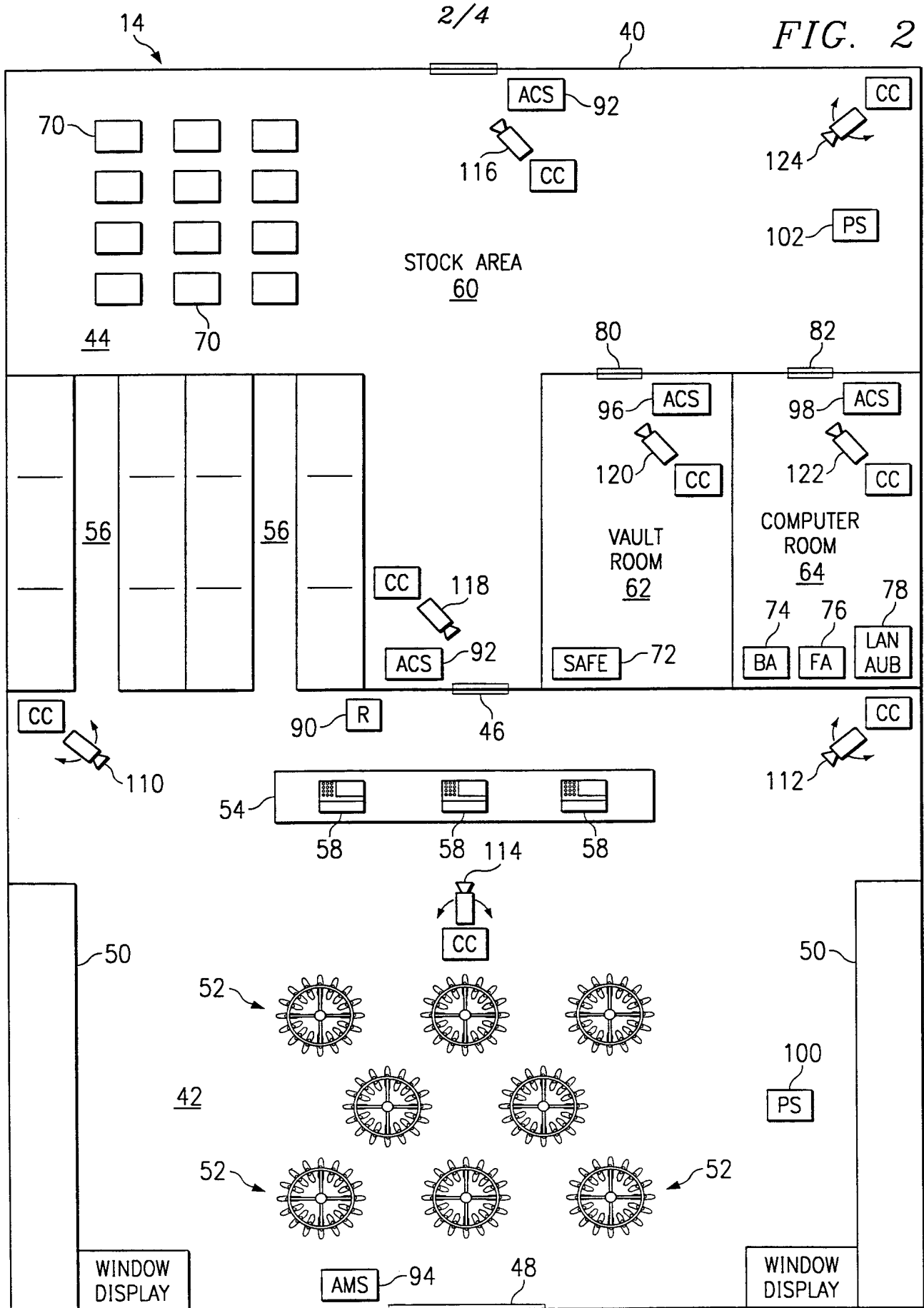
27. The method of Claim 25, the act of receiving a request comprising eliciting a radio response from a radio frequency identification (RFID) tag at an access door to the restricted area and the act of transmitting
20 the request including transmitting the radio response from the RFID tag.

1/4



2/4

FIG. 2



3/4

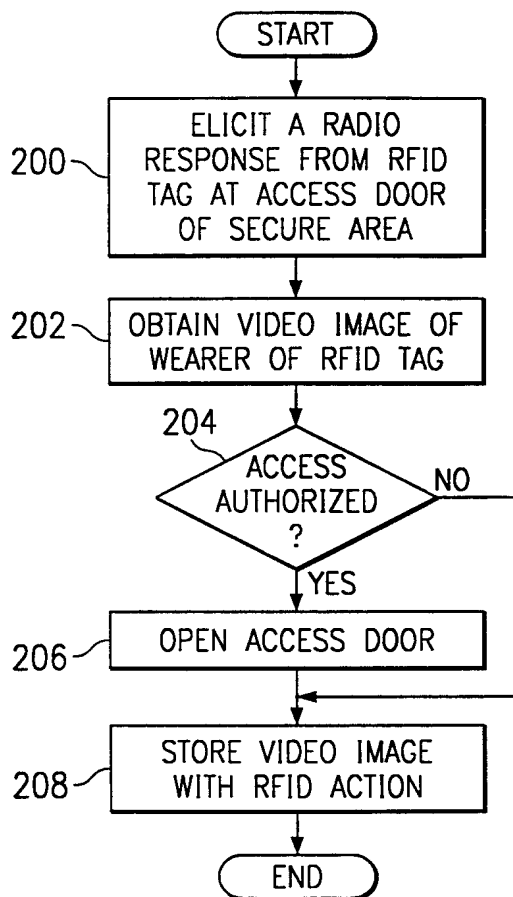


FIG. 4

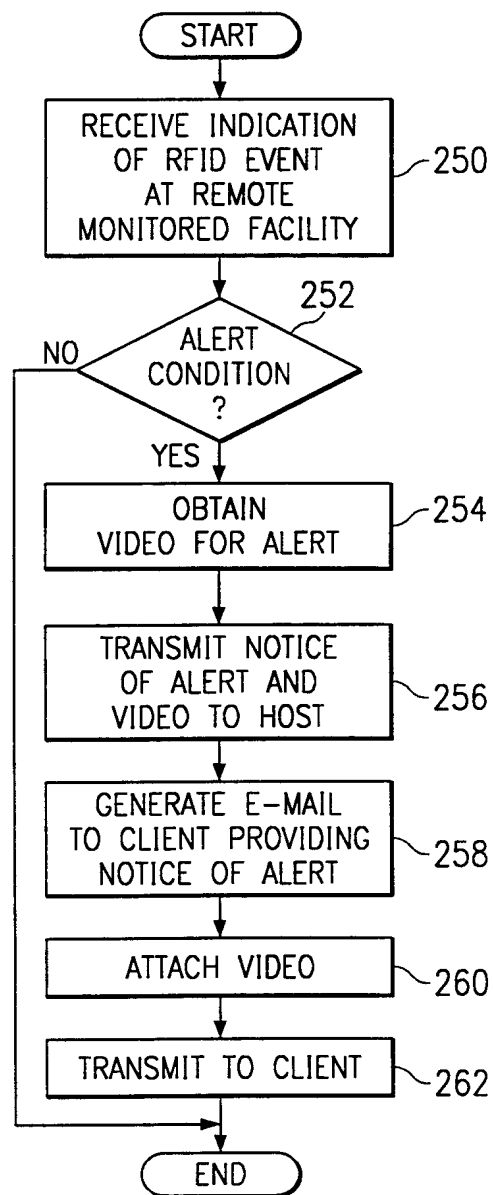


FIG. 5

4/4

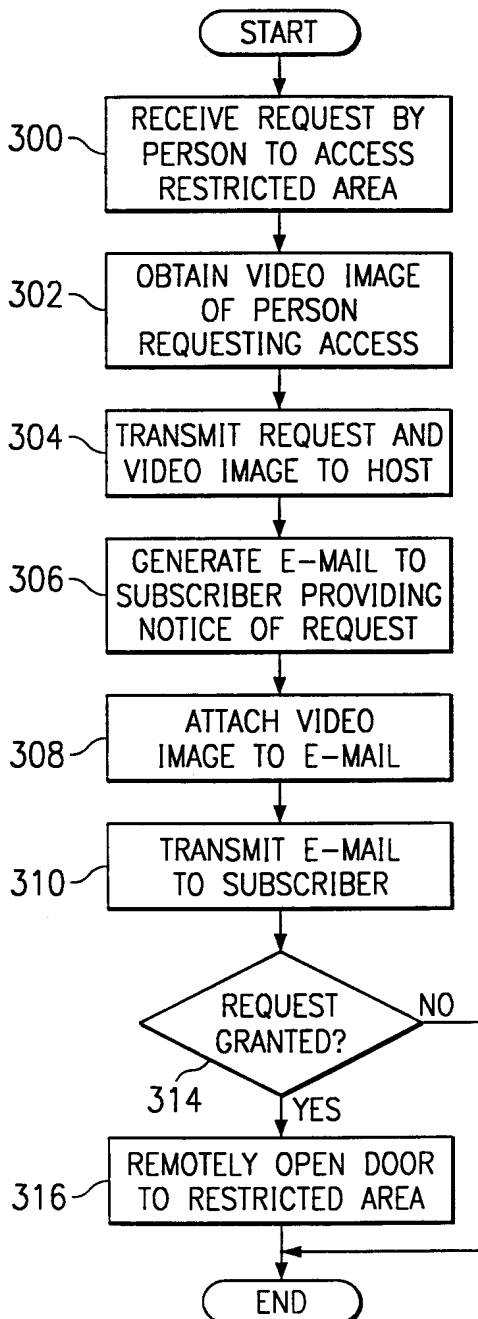


FIG. 6

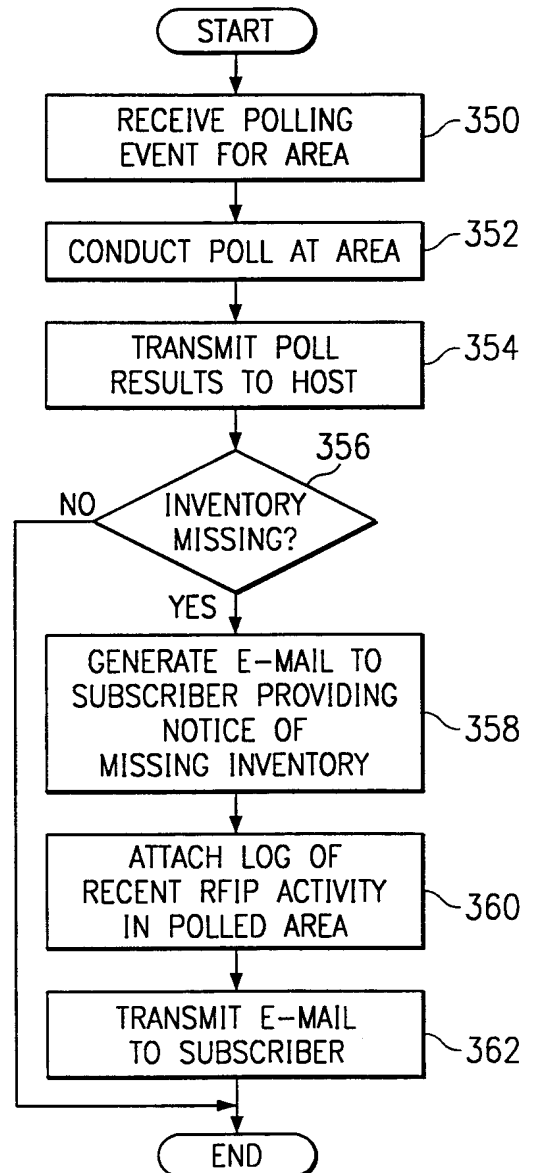


FIG. 7

INTERNATIONAL SEARCH REPORT

Inte. .ional Application No

PCT/US 00/42802

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G08B13/24 G08B15/00 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G08B G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 11520 A (CHECKPOINT SYSTEMS INC) 19 March 1998 (1998-03-19)	1-7
Y	abstract	8-14
Y	WO 95 12858 A (GEN HOSPITAL CORP ;BAXTER INT (US)) 11 May 1995 (1995-05-11) abstract	8-13
X	US 5 321 396 A (LAMMING MICHAEL G ET AL) 14 June 1994 (1994-06-14)	15-27
Y	the whole document	14
X	US 5 432 864 A (LU DAOZHENG ET AL) 11 July 1995 (1995-07-11) abstract	15-27
	--- -/-	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

A document defining the general state of the art which is not considered to be of particular relevance

E earlier document but published on or after the international filing date

L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

O document referring to an oral disclosure, use, exhibition or other means

P document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

* & * document member of the same patent family

Date of the actual completion of the international search

11 May 2001

Date of mailing of the international search report

18/05/2001

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Sgura, S

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 00/42802

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 689 442 A (MOEN JERRY M ET AL) 18 November 1997 (1997-11-18) column 3, line 35 -column 4, line 13; figure 1	1
A	DE 298 15 797 U (SIEMENS) 29 October 1998 (1998-10-29) claims 1,2; figure 1	1-5

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 00/42802

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9811520 A	19-03-1998	US 5745036 A AU 716240 B AU 4079197 A CN 1230270 A EP 0928468 A JP 2001501328 T	28-04-1998 24-02-2000 02-04-1998 29-09-1999 14-07-1999 30-01-2001
WO 9512858 A	11-05-1995	US 5434775 A AU 686269 B AU 8097394 A CA 2152276 A EP 0685090 A JP 8508359 T	18-07-1995 05-02-1998 23-05-1995 11-05-1995 06-12-1995 03-09-1996
US 5321396 A	14-06-1994	NONE	
US 5432864 A	11-07-1995	NONE	
US 5689442 A	18-11-1997	WO 9912354 A AU 4238297 A	11-03-1999 22-03-1999
DE 29815797 U	29-10-1998	NONE	